Statement of Ambassador Linton F. Brooks
Under Secretary of Energy for Nuclear Security and
Administrator, National Nuclear Security Administration
Before the
Committee on Energy and Commerce
Subcommittee on Oversight and Investigations
United States House of Representatives

June 9, 2006

Good morning, Mr. Chairman, thank you for the opportunity to appear before you today in support of the Department's efforts to strengthen our cyber security.

The National Nuclear Security Administration Act (NNSA) established the NNSA within the Department of Energy (DOE) with the mission to strengthen the United States' security through the military application of nuclear energy and by reducing the global threat from terrorism and weapons of mass destruction. As Administrator, one of my duties is the security of NNSA's information systems and networks.

NNSA is responsible for the majority of the classified networks within the Department and we take this responsibility very seriously. Our classified networks receive our highest priority and we have taken all possible steps to ensure their security. I am confident of the security of our classified systems and networks and to date we have been successful in preventing any breach in security. However, we must maintain constant vigilance over the systems entrusted to us and it is essential that we continue the improvements underway to upgrade the infrastructure and improve integration across the Federal complex. Only by doing so can we ensure the long-term cyber security of the nuclear weapons complex.

NNSA is dependent upon information and upon the systems that create, process, store, and communicate information to carry out our missions. But the management of the security for these systems must rely on a comprehensive understanding of systems, in depth analyses of every new attack, and a timely determination of the best approach to mitigate the efforts of intruders. Doing so requires a substantial commitment of resources-- both financial and intellectual—and a coordinated effort across all elements of the Department.

I look to Mr. Tom Pyke, Chief Information Office (CIO) for the Department, to integrate our Departmental efforts. NNSA supports the Federated approach and is applying that approach across the NNSA complex. We have engaged each of our laboratories, plants, sites and offices in assessing the priorities that must be addressed in the future. These priorities are based on the risks at each site, as each site has different types of information it must protect and transmit.

Cyber security threats are increasing in complexity and number and we are working to strengthen our cyber security posture. We continue to monitor all aspects of cyber

security throughout the NNSA complex and to apply risk management to balance cyber security issues with available budget resources. NNSA, with leadership from the CIO, is working closely with the Office of Security and the Office of Counterintelligence to maintain awareness of cyber security threats. We are jointly working to maximize our efforts and resources to ensure a secure environment for the transmission and storage of our information.

Today, I would like to highlight four specific efforts that benefit the department and strengthen cyber security throughout the weapons complex:

Diskless Workstation Upgrades: Plans are in place to convert the department's classified workstations to diskless operations. The plans support the completion of the conversion effort by the end of FY 2008 and as of the end of April 2006 over 45% of the Department's classified workstations were operating without disks. The ultimate success of the effort is tightly linked to the ability of the Integrated Cyber Security Initiative (ICSI) to implement a gateway to permit non-weapons data – both DOE and other agency data – to traverse the Department utilizing the Enterprise Secure Network. Development work on the gateway, including a connection to SIPRNet, is expected to begin in FY 2007.

Continuous Asset Monitoring System (CAMS): CAMS has two overarching objectives: 1) to improve security monitoring of DOE's and NNSA's networks (both classified and unclassified) in near real-time as well as software patch management; and 2) to increase the efficiency and accuracy of congressionally-mandated, asset-based reporting. A joint NNSA-DOE team invested almost 18 months testing and evaluating multiple vendors' offerings with the goal of selecting a common solution for both classified and unclassified operational environments, to minimize cost and standardize the system administration. To meet the Agency's long term reporting obligations, a customized architecture was selected consisting of hardware, software and process solutions which will be implemented across the Department and will include all NNSA sites, labs, plants and offices.

Encrypted Communication: With the support of Congress, we have accelerated deployment of enterprise encryption for secure authentication and communication. We fully support the Department's move to purchase encryption software. Currently, NNSA and DOE have multiple contracts. An agreement is being negotiated where these licenses will be combined into a single agreement and upgraded to a new thin client version. New licenses will be purchased at a reduced rate as needed. This combined arrangement will ultimately save the Department over one million dollars in licensing and maintenance costs.

Cyber Security Training: NNSA has partnered with DOE in a training working group that evaluates products and vendors training programs for all positions in the management and use of computing assets. Training for our cyber security professionals is also key to raising awareness and acceptance of assessing and prioritizing cyber security risks at all sites.

NNSA has also developed a comprehensive set of cyber security policies that standardize the configuration of many of our systems and assists in fully documenting the risks associated with the certification and accreditation of our computing assets. The policies we have directed fully implement national and federal policies in a graded risk management approach. Site managers now have a uniform risk acceptance based process for assessing requirements and for implementing their cyber security programs.

NNSA is moving forward on multiple fronts to strengthen and ensure a safe information technology working environment. We continue to report our Office of Management and Budget (OMB) cyber security metrics and actively use this information to improve program control and evaluation. We continue to develop our continuity of operations plans as required by Departmental directives. We have established a working group to improve our cyber security by establishing security configurations for each of the computer systems in use across our federal and contractor sites. NNSA is teaching classes in cyber security policy implementation that expand on the DOE information as required for our weapons complex. Finally, we continue to support the Department to improve the inventory of our information systems.

Mr. Chairman, we are working diligently to maintain a secure environment for our information and that of the Department. We are moving ahead, we are making progress, and with the Federated approach, and we will be able to better manage risk and the efficient use of resources.

I look forward to your questions. Thank you.